Chapter 18

ISDN

Topics Covered

Introduction to ISDN network
ISDN network architecture
Configuration of ISDN Circuits
ISDN DDR configuration
Troubleshooting ISDN network

visioninfosystems@vsnl.net

Integrated Services Digital Network

ISDN is a digital circuit-switched service provided by telecommunications providers (Telephone Company) to allow voice, data, and video and audio transmissions over existing digital telephone lines. ISDN is often used as a low cost alternative to Frame Relay or T1 connections while still offering a higher connection speed than an analog modem. ISDN was designed to over the problem faced by PSTN service

Difference between PSTN and ISDN

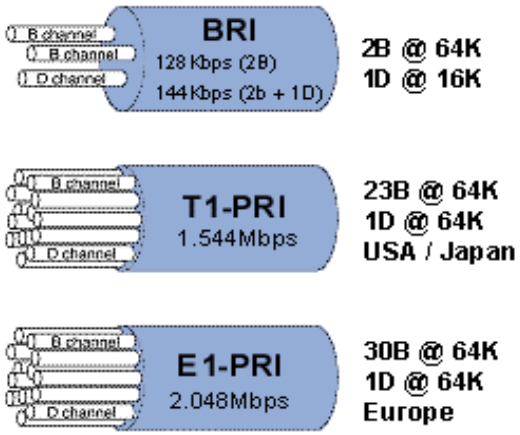
PSTN (Public Switched Telephone Network)	ISDN (Integrated Service Digital Network)
Analog Transmission	Digital Transmission
Designed only for Voice transmission	Designed for Voice, Video and Data
No channels	Channels
56 kbps speed	64 + 64 kbps speed (2B+1D)
Required PSTN based v.34 or v.90 modem for digital to analog conversion.	Required TA (Terminal Adapter) with NT box for connectivity.

ISDN service:

- **Basic Rate Interface (BRI)**
- **Primary Rate Interface (PRI)**

BRI is normally used in small offices or for home connections whereas PRI is used in larger network environments because it provides higher bandwidth and multiple channels. PRI is also used at HUB or Central location where as ISDN lines are terminated.

ISDN Channels



Teleco providers offer digital connections via ISDN as channels, BRI connections offer three channels: two at 64Kbps and one at 16Kbps for a maximum throughput of 128Kbps. The 64K channels are known as bearer or B-channels because they carry the data for the connection. ISDN BRI connections use the 16Kbps-signaling channel, which is also called the D-channel, to control the communications on the link. PRI connections offer 23 B-channels and one 64Kbps D-channel for a bit rate of up to 1.544Mbps. European ISDN PRI service offers 30 64Kbps B-channels and one 64Kbps D-channel yielding a total

interface rate of 2.048Mbps. In both ISDN BRI and PRI, a single D-channel is used for signaling information, and the B-channels are used to carry the data. Because the control communications are conducted on a channel that is separate from the data transfer, ISDN is said to be out of band signaling.

ISDN can be used to:

- Add bandwidth for telecommuting.
- Improve Internet response times.
- Carry multiple Network layer protocols.
- Encapsulate other WAN services.
- Provide Voice, Video and Data services
- Pure digital transmission

ISDN Standards

ISDN is referenced by a suite of ITU-T (International Telecommunications Union) standards that encompass the OSI model's Physical, Data Link, and Network layers. The ISDN standard defines the hardware and call-setup scheme for end-to-end digital connectivity. The standards are grouped into ITU-T groups and are organized into three letter designations: I, E, and Q. Then each group is subdivided into specific protocols, preceded by the group designator.

ISDN Protocol Series		
Protocol Series	**Description**	**Examples**
E	Telephone and network standards	E.163 - Telephone numbering E.164 ISDN addressing
I	Methods, terminology, concepts, and interfaces	I.100 - Terminology, structure, and concepts I.300 - Networking recommendations
Q	Signaling and switching standards	Q.921 - Data Link layer LAPD procedures Q.931 - Network layer functions

ISDN Operations

Link Access Procedure, D channel

Layer 2 of the ISDN signaling protocol is Link Access Procedure, D channel, also known as LAPD, it is used by ISDN to pass the signaling messages between the router and the ISDN switch at the local CO. LAPD is similar to High-Level Data Link Control (HDLC) and Link Access Procedure, Balanced (LAPB). As the expansion of the LAPD acronym indicates, it is used across the D channel to ensure that control and signaling information flows and is received properly. The data travels between routers on the

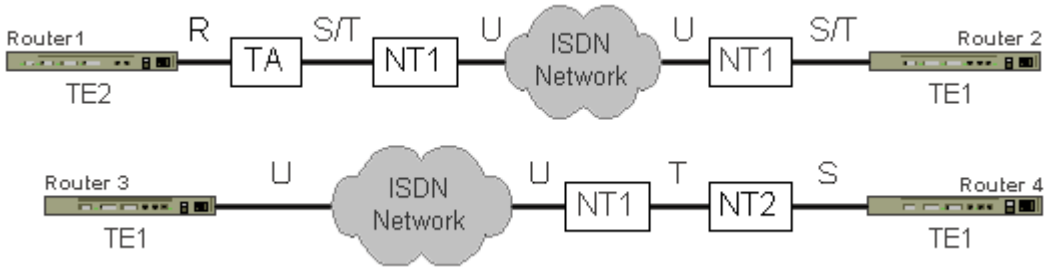
B-channels via HDLC or PPP encapsulation. The LAPD frame format is very similar to that of HDLC and, like HDLC, LAPD uses supervisory, information, and unnumbered frames. The LAPD protocol is formally specified in ITU-T Q.920 and ITU-T Q.921.

ISDN Components

ISDN standards use function groups and reference points to describe the various components that can be utilized in making an ISDN connection. Function groups describe a set of functions that are implemented by a device and software.

In the figure below, Router 1 is a router without a BRI interface so it uses a TA (ISDN Modem) to connect to the ISDN line. Router 2 has a BRI interface without a built-in NT1. Router 3 has a BRI interface with a built-in NT1. Router 4 is attached to a line that uses a NT2 device for the local PBX.

Function Groups and Reference Points



Functions represent devices or hardware function within ISDN.

ISDN Functions and Devices

- **Terminal Adapter (TA)** --- A converter device that allows non-ISDN devices to operate on an ISDN network.
- **Terminal Equipment 1 (TE1)** --- A device that supports ISDN standards and that can be connected directly to an ISDN network connection. For example, routers with integrated ISDN interfaces, ISDN telephones, personal computers, or videophones could function as TE1s.
- **Terminal Equipment 2 (TE2)** --- A non-ISDN device, such as a router, analog phone or modem, which requires a TA in order to connect to an ISDN network.
- **Network Termination 1 (NT1)** --- A small connection box that is attached to ISDN BRI lines. This device terminates the connection from the Central Office (CO). Converts BRI signals for use by ISDN line.
- **Network Termination 2 (NT2)** --- A device that provides switching services for the internal network. This type of interface is typically used with PRI lines, when they need to be divided for several functions. For example, some channels may be used for WAN data communications and others for the telephone system (such as PBX) and/or video tele-conferencing. It is a more complex NT1 that performs layer 2 and 3 functions.

The connection between two function groups (including cabling) is called a reference point.

ISDN Reference Points

- **U** --- The **U-interface** is the actual two-wire cable, also called the local loop that connects the Customer Premise Equipment to the telecommunications provider.
- **R** --- The **R-interface** is the wire or circuit that connects the TE2 to the TA.
- **S** --- The **S-interface** is a four-wire cable from TE1 or TA to the NT1 or NT2, which is a two-wire termination point.
- **T** --- The point between the NT1 and NT2, is the T-interface. This four-wire cable is used to divide the normal telephone company's two-wire cable into four-wires, which then allows the connection of up to eight ISDN devices.
- **S/T** --- When NT2 is not used on a connection that uses NT1, the connection from the router or TA to the NT1 connection is typically called S/T. This is essentially the combination of the S and T reference points.

Configuring ISDN on Cisco Routers

Accessing ISDN with a Cisco router means that you will need to purchase either a Cisco router with a built-in NT1 (U reference point) or an ISDN modem (called a TA). If your router has a BRI interface (called a TE1), you only need attach an NT1 device to connect to the services. If your router doesn't have a BRI interface (called a TE2), you need to attach a TA and a NT1 to connect to ISDN services.

ISDN supports virtually every upper layer protocol (IP, IPX, AppleTalk), and you can choose PPP, HDLC, or X.25 as the encapsulation protocol.

ISDN Switch Types

To configure a router for the variety of switches it's going to connect to, use the command:

Router(config)#isdn switch-type [*identifier*]

Supported Switch Types	
Identifier	**Description**
`basic-nil`	AT&T basic rate switches
`basic-5ess`	AT&T 5ESS basic rate switches
`basic-dms100`	Nortel DMS-100 basic rate switches
`basic-4ess`	AT&T 4ESS primary rate switches
`primary-5ess`	AT&T 5ESS primary rate switches
`primary-dms100`	Nortel DMS-100 primary rate switches
`vn2`	French VN2 ISDN switches
`vn3`	French VN3 ISDN switches
`ntt`	Japanese NTT ISDN switches
`basic-1tr6`	German 1TR6 ISDN switches

Service Profile Identifiers (SPIDs)

A service profile identifier (SPID) is a number provided by the ISDN carrier to identify the line configuration of the BRI service. SPIDs allow multiple ISDN devices, such as voice and data, to share the local loop. Each SPID points to line setup and configuration information. SPIDs are frequently referred to as ISDN phone numbers because their functions are the same. An ISDN device can access each ISDN channel via its SPID number. You can configure the router to utilize a single or multiple SPIDs when making a connection to the ISDN provider.

When a device attempts to connect to the ISDN network, it performs a D channel Layer 2 initialization process that causes a TEI to be assigned to the device. The device then attempts D channel Layer 3 initialization. If SPIDs are necessary but not configured or configured incorrectly on the device, the Layer 3 initialization fails, and the ISDN services cannot be used.

The ISDN provider must assign the SPID numbers for each channel, which is usually an 8 to 14 digit number. There is no standard format for SPID numbers. As a result, SPID numbers vary depending on the switch vendor and the carrier. You can then use those numbers to configure your ISDN dialer connections. You must also identify the type of switch that is used at the CO to which you are connecting. The following commands show an ISDN BRI connection (two SPIDS for 2 B-channels):

```
Router3(config)#isdn switch-type dms-100
Router3(config)#interface bri 0
Router3(config-if)#isdn spid1 52069145231010
Router3(config-if)#isdn spid2 52069145241010
```

If you want your Cisco router to answer incoming calls over your ISDN line, you can configure an ISDN sub-address by specifying the local directory number (LDN), which is the seven-digit number assigned by the service provider and used for call routing. The LDN is not necessary for establishing ISDN-based connections, but it must be specified if you want to receive incoming calls on B channel 2. The LDN is required only when two SPIDs are configured (for example, when connecting to a DMS or NI1 switch). Each SPID is associated with an LDN. Configuring the LDN causes incoming calls to B channel 2 to be answered properly. If the LDN is not configured, incoming calls to B channel 2 may fail. The following commands configure LDNs for an ISDN BRI link:

```
Router3(config)#interface bri0
Router3(config-if)#isdn spid1 0835866201 8358662
Router3(config-if)#isdn spid2 0835866401 8358664
```

Configure Called Party Number Verification

When multiple devices are attached to an ISDN BRI, you can ensure that only a single device answers an incoming call by verifying the number or sub-address in the incoming call against the device's configured number or sub-address or both. You can specify that the router verify a called-party number or sub-address number in the incoming setup message for ISDN BRI calls, if the number is delivered by the switch. You can do so by configuring the number that is allowed. To configure verification, use the following command in interface configuration mode:

isdn answer1 [*called-party-number*][:sub-address]

Verifying the called-party number ensures that only the desired router responds to an incoming call. If you want to allow an additional number for the router, you can configure it, too. To configure a second number to be allowed, use the following command in interface configuration mode:

isdn answer2 [*called-party-number*][:sub-address]

Dial on Demand Routing (DDR)

Dial-on-demand routing (DDR), is used to allow two or more Cisco routers to dial an ISDN dial-up connection on an as-needed basis. DDR is only used for low-volume, periodic network connections using either a PSTN or ISDN. This was designed to reduce WAN cost if you have to pay on a per-minute or per-packet basis. DDR configuration commands define host and ISDN connection information. An access list and DDR dialer group define what kind of traffic should initiate an ISDN call. You can configure multiple access lists to look for different types of interesting traffic. Interesting traffic is traffic that (when it arrives at the router) triggers the router to initiate the ISDN connection.

When a router notices interesting traffic, it refers to its ISDN information and initiates setup of the ISDN call through its BRI or PRI and NT1 devices. When a connection is established, normal routing occurs between the two end devices. After interesting traffic stops being transmitted over the ISDN connection, the connection idle timer begins. When the idle timer expires, the connection is terminated.

Steps of how DDR works

1. Route to the destination network is determined.
2. Interesting packet dictates a DDR call.
3. Dialer information is looked up and connection is made.
4. Traffic is transmitted.
5. Call is terminated when no more traffic is being transmitted over a link and the idle-timeout period ends.

Configuring a DDR connection

```
Router3(config-if)#dial wait-for-carrier time 15
Router3(config-if)#dialer idle-timeout 300
Router3(config-if)#dialer load-threshold 50 either
Router3(config-if)#dialer map ip 192.168.52.1 name CORP speed 56 5205551212
```

The first command tells the dialer to wait no longer that 15 seconds for the ISDN provider to answer during a DDR connection attempt. The second command tells the dialer to hang-up the connection if the connection does not pass any interesting information for 300 seconds (default is 120 seconds). The third command tells the dialer to only dial additional lines (assuming you have configured multiple ISDN channels for the connection) when any channel is transferring at 50% of the available bandwidth, either inbound or outbound. The fourth command maps the dialer to a specific hostname (CORP), IP address (192.168.52.1), speed (56Kbps, default is 64Kbps if not specified), and phone number (5205551212).

Dialer Map Entries

Dialer map statements relate upper layer addresses to their associated phone numbers.

Specifying Interesting Traffic

In order to define what type of traffic is considered interesting and will in turn bring up the ISDN line, you must use dialer group commands. The following commands show how to use a dialer group and access lists to permit IP traffic on your link, but deny IGRP traffic. The **dialer list** global configuration command defines the interesting packets, and the **dialer group** command sets the access list on the BRI interface.

```
Router3(config)#dialer-list 1 protocol ip list 110
Router3(config)#access-list 110 deny igrp any any
Router3(config)#access-list 110 permit ip any any
Router3(config)#int bri0
Router3(config-if)#dialer-group 1
```

Access lists are used in ISDN connections to prevent specified traffic from initiating a connection. To control connections, traffic that is desired on the ISDN connection is allowed while everything else is denied.

Encapsulation Methods

When a clear Data Link is established between two DDR peers, internetworking datagram's must be encapsulated and framed for transport across the Dialer media. The encapsulation methods available depend on the physical interface being used. Cisco supports the following encapsulations for DDR:

- **PPP** -- is the recommended encapsulation method because it supports multiple protocols and is used for synchronous, asynchronous, or ISDN connections. In addition, PPP performs address negotiation and authentication and is supported by multiple vendors.
- **HDLC** -- is supported on synchronous serial lines and ISDN connections only. HDLC supports multiple protocols, but it doesn't provide authentication.
- **SLIP** -- works on asynchronous interfaces only, and is supported by IP only. Addresses must be configured manually, it doesn't provide authentication, and is interoperable only with other vendors that use SLIP.
- **X.25** -- is supported on synchronous serial lines and a single ISDN B channel.

PPP Authentication

- **Password Authentication Protocol (PAP)**
  PAP provides a simple method for a remote node to establish its identity using a two-way handshake. This is done only upon initial link establishment. After the PPP link establishment phase is complete, a username/password pair is repeatedly sent by the remote node until authentication is acknowledged, or the connection is terminated.

  Passwords are sent across the link in plain text and there is no protection from playback or trail-and-error attacks. The remote node is in control of the frequency and timing of the login attempts. If the local host rejects the username/password, the connection is terminated.

- **Challenge and Handshake Protocol (CHAP)**
  CHAP is used to periodically verify the identity of the remote node using a 3-way handshake. This is done upon initial link establishment and can be repeated any time after the link has been established. After the PPP link establishment phase is complete, the host sends a challenge messages to the remote node. The remote node responds with a value calculated using a one-way

hash function (typically MD5). The host checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. Otherwise, the connection is terminated.

CHAP provides protection against playback attack through the use of a variable challenge value that is unique and unpredictable. The use of repeated challenges is intended to limit the time of exposure to any single attack. The host is in control of the frequency and timing of the challenges.

ISDN Configuration Example

This is an example of a connection between a corporate headquarters and a remote site over a BRI ISDN link.

Remote Network
Router Configuration: **Name**:REMOTE **E0 IP address**:192.168.24.1 **Local Network**:192.168.24.0 **BRI 0 IP address:**192.168.49.2
REMOTE(config)#hostname corp password 123pass332 **REMOTE(config)#isdn switch-type dms-100** **REMOTE(config)#interface bri 0** **REMOTE(config-if)#encapsulation ppp** **REMOTE(config-if)#ppp authentication chap** **REMOTE(config-if)#spid1 5208881111 5270936** **REMOTE(config-if)#spid2 5208881212 5270956** **REMOTE(config-if)#ip address 192.168.49.2 255.255.255.0** **REMOTE(config-if)#dialer idle-timeout 600** **REMOTE(config-if)#dialer map ip 192.168.49.1 name corp 7045551212** **REMOTE(config-if)#dialer load-threshold 125 either** **REMOTE(config-if)#ppp multilink** **REMOTE(config-if)#dialer-group 1** **REMOTE(config-if)#exit** **REMOTE(config)#dialer-list 1 protocol ip permit** **REMOTE(config)#ip route 0.0.0.0 0.0.0.0 192.168.49.1** **REMOTE(config)#ip route 192.168.49.0 255.255.255.0 192.168.49.1**
Corporate network
Router Configuration: **Name**:CORP **BRI 1 IP address:**192.168.49.1
CORP(config)#hostname remote password 123pass332 **CORP(config)#isdn switch-type dms-100** **CORP(config)#interface bri 1** **CORP(config-if)#encapsulation ppp** **CORP(config-if)#ppp authentication chap** **CORP(config-if)#spid1 7047773333 5265933**

```
CORP(config-if)#spid2 7047774444 5265944
CORP(config-if)#ip address 192.168.49.1 255.255.255.0
CORP(config-if)#dialer idle-timeout 600
CORP(config-if)#dialer map ip 192.168.49.2 name remote 5205551212
CORP(config-if)#dialer load-threshold 125 either
CORP(config-if)#ppp multilink
CORP(config-if)#dialer-group 1
CORP(config-if)#exit
CORP(config)#ip route 192.168.24.0 255.255.255.0 192.168.49.2
CORP(config)#dialer-list 1 protocol ip list 110
CORP(config)#access-list 110 deny igrp any any
CORP(config)#access-list 110 permit ip any any
```

The routers are both using PPP encapsulation and CHAP authentication. The username has been set for the opposite router in each configuration and the password is the same on both. Each router has the ability to dial the other. The CORP router is located at the corporate network, which has other connections and uses IGRP to transfer routing tables on the corporate network. However, IGRP is not desired on the ISDN connection, so the CORP router has an access list specifically denying IGRP on the ISDN link. Both routers permit all IP traffic on the ISDN link and all IP traffic will be considered interesting or worth activating the ISDN link for. Multilink is enabled on both routers, and they will dial their additional lines when there is 50% (load-threshold uses a number between 1 and 255, with 255 being 100%) or more utilization on the first channel. The link will be terminated if there is no interesting traffic for 600 seconds (10 minutes). The IP routes are configured such that all traffic destined from the corporate network to 192.168.24.0 will be sent to the REMOTE router. Since the REMOTE router is a remote branch with no other connections, all traffic that is not specifically destined for 192.168.24.0 will be sent to the CORP router. Note that each router has its dialer mapped to the IP address of the other router.

Troubleshooting and Monitoring ISDN

All commands are available via privileged EXEC mode prompt (enable mode)

- **`clear interface bri [#]`** --- Resets the counters and terminates the connection.
- **`show dialer`** --- Reports information regarding the DDR connection including the number dialed, the success of the connection, the idle timers, and the number of calls that were rejected due to administrative policy.
- **`show ip route`** --- Show all routes the router knows about.
- **`show isdn active`** --- Displays the status of the ISDN connection while the call is in progress.
- **`show isdn status`** --- Gives status information for ISDN connections.
- **`show interface bri 0`** --- Shows you the configuration statistics and speed of your ISDN BRI interface.
- **`show controllers bri 0`** --- Shows detailed information about the B and D channels.
- **`debug dialer`** --- Shows information regarding the cause of a dialing connection and the status of the connection.
- **`debug bri`** --- Provides information about the B channels of the BRI.

- **`debug isdn q921`** --- Used to see layer-2 information. Shows information regarding the D-channel interface. The D-channel is always connected. Connections over the B-channel can't occur without signaling over the D-channel.
- **`debug isdn q931`** --- Shows the call setup and teardown. Output can be used to verify acknowledgments and messages. [layer 3 on D-channel]
- **`no debug all`** --- Use to turn off all debugging.